認定 NPO 法人スペシャルオリンピックス日本・神奈川

# 個人情報保護規程

## 第 1 章　総則

（目的）

第 1 条　本規程は、認定 NPO 法人スペシャルオリンピックス日本・神奈川(以下、「当法人」という）の役職員が遵守すべき個人情報の取扱いに関する必要事項を定め、個人の権利利益を保護し、当法人が保有する個人情報(以下、「保有個人情報」という)の適切な管理のために必要な措置について定めるものとする。

（定義）

第 2 条　本規程において、次の号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1)個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

(2) 保有個人情報

役職員等が職務上作成し、又は取得した個人情報を含む情報の集合物であって、役職員等が組織的に利用するものとして、当法人が保有しているものをいう。

（適用範囲）

第 3 条　本規程は、当法人のすべての役職員等に適用する。また、退職後においても在任又は在籍中に取得・アクセスした個人情報については、本規程に従うものとする。

2　「役職員等」とは、当法人に属するすべての理事、監事および職員をいう。

3　専門委員、各種委員会委員、顧問 、相談役及び当法人の事業について委嘱または依頼を受けた者が、当法人の業務に従事する場合は、当該従事者は本規程を遵守しなければならない 。

4　前項の従事者を管理する立場にある者は、当該従事者に対して 本規程の遵守を確保するために必要な措置を講じなければならない。

## 第 2 章 管理体制

（総括保護管理者）

第 4 条　当法人に、総括保護管理者 1 名を置く。

2　総括保護管理者は、事務局担当理事をもって充てる。

3　総括保護管理者は、次に掲げる事務を行うものとする。

(1)保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うために必要があると認めるときは、関係職員を構成員とする委員会等を設け、定期又は随時に開催すること。

(2) 前号に掲げるもののほか、当法人における保有個人情報の管理に関する事務の総括に係わること。

(保護管理者)

第５条　当法人に、保護管理者１名を置く。

2　保護管理者は、事務局長をもって充てる。

3　保護管理者は、総括保護管理者の指示に従い、事務局における保有個人情報の管理に関する事務を行う。

(システム管理者)

第７条　総括保護管理者が指定するシステム管理者を当法人に若干名置き、システム管理者は、保有個人情報がその目的に沿って適切に使用され、必要なアクセス（情報に接する行為をいう。以下同じ。)ができるように情報システムの構築、管理、運用及びセキュリティ対策等に関する事務を行う。

(個人情報保護に関する担当窓口)

第８条　当法人の個人情報保護に関する取りまとめは、事務局が行うものとし、責任者として、事務局長をもって充てることとし、次に掲げる事務を行うものとする。

(1)個人情報の取扱いに対する問合せ、相談、苦情等への対応

(2) 開示及び訂正の請求又は利用停止請求の受付及び開示請求等をしようとする者への対応

（監査責任者）

第９条　当法人に、監査責任者１名を置く。

2　監査責任者は、会長が指名する役職員とする。

3　監査責任者は、当法人における保有個人情報の管理の状況について監査する。

（研修))

第１０条　総括保護管理者は、保有個人情報の取扱いに従事する職員に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行うものとする。

2　総括保護管理者は、保有個人情報の適切な管理のため、システム管理者に対し、情報システムの構築、管理、運用及びセキュリティ対策等に関して必要な教育研修を行うものとする。

3　保護管理者は、保有個人情報の適切な管理のため、職員に対し、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。

## 第３章 職員の責務

（職員の責務))

第１１条　職員は、法令、本規程及び個人情報保護管理マニュアル、並びに総括保護管理者、保護管理者、システム管理者の指示に従い、保有個人情報を取り扱わなければならない。

## 第４章 保有個人情報の取扱い

(アクセス制限)

第１２条　保護管理者は、保有個人情報の重要度に応じて、保有個人情報にアクセスをする権限(以下「アクセス権限」という。)を有する者を、保有個人情報の利用目的を達成するために必要最小限の職員に限定するものとする。

２　アクセス権限を有しない職員は、保有個人情報にアクセスをしてはならない。

３　職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスをしてはならない。

(複製等の制限)

第１３条　職員は、業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行うものとする。

(1) 保有個人情報の複製及び送信

(2) 保有個人情報が記録されている媒体の外部への送付又は持ち出し

(3) その他、保有個人情報の適切な管理に支障を及ぼす恐れのある行為として、保護管理者が定めるもの

(誤りの訂正等)

第１４条　職員は、保有個人情報の訂正を行う場合には、保護管理者の指示に従うこととし、保護管理者は、重要度に応じて、総括保護管理者に報告を行うなど必要な措置を講ずるものとする。

（媒体の管理等))

第１５条　職員は、保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管するとともに、保護管理者が必要があると認めるときは、当該媒体を耐火金庫等へ保管するなど、保有個人情報の漏えい、滅失又は毀損を防止するための措置を講ずるものとする。

(廃棄)

第１６条　職員は、保有個人情報又は保有個人情報が記録されている媒体(端末機器及びサーバー内に内蔵されているものを含む。)が不要となった場合には、保護管理者の指示に従い、個人情報の復元又は判読が不可能な方法により、当該情報の消去又は当該媒体の廃棄を行うものとする。

(保有個人情報の取扱い状況の記録)

第１７条　保護管理者は、保有個人情報の重要度に応じて、台帳を整備し、保有個人情報の利用、保管等の取扱いの状況について記録するものとする。

## 第５章 情報システムにおける安全の確保等

(アクセス制御)

第１８条　保護管理者及びシステム管理者は、保有個人情報（情報システムで取り扱うものに限る。以下この章及び次章において同じ。)の重要度に応じて、パスワード等を使用してアクセス権限を識別するする機能(以下「承認機能」という。)を設定するなど、保有個人情報へのアクセスを制御するために必要な措置を講ずるものとする。

２　保護管理者及びシステム管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備(その定期又は随時の見直しを含む。)し、パスワード等の読取防止等に必要な措置を講ずるものとする。

（外部からの不正アクセスの防止）

第２０条　保護管理者及びシステム管理者は、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアーウォールの設定による経路制御等の必要な措置を講ずるものとする。

(コンピュータウイルスによる漏えい等の防止)

第２１条　保護管理者及びシステム管理者は、コンピュータウイルスによる保有個人情報の漏えい、滅失又は毀損の防止のため、コンピュータウイルスの感染防止等に必要な措置を講ずるものとする。

(暗号化)

第２２条　保護管理者及びシステム管理者は、保有個人情報の重要度に応じて、その暗号化のために必要な措置を講ずるものとする。

(バックアップ)

第２３条　保護管理者及びシステム管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散管理するために必要な措置を講ずるものとする。

(情報システム設計書等の管理)

第２４条　保護管理者及びシステム管理者は、保有個人情報に関する情報システムの設計書、構成図等の文書について、外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

(端末機器の限定)

第２５条　保護管理者及びシステム管理者は、保有個人情報の重要度に応じて、保有個人情報の処理を行う端末機器を限定するために必要な措置を講ずるものとする。

(端末機器の盗難防止等)

第２６条　保護管理者及びシステム管理者は、端末機器の盗難又は紛失の防止に関する必要な措置を講

ずるものとする。

2　職員は、保護管理者及びシステム管理者が必要であると認めるとき以外は、端末機器を外部へ持ち出し、又は外部から持ち込んではならない。

（閲覧防止）

第２７条　職員は、端末機器の使用に当たっては、保有個人情報が当法人職員以外の者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずるものとする。

(情報システムの安全管理)

第２８条　保有個人情報を取扱う基幹的なサーバー等、情報システムの安全管理責任者は、システム管理者をもって充てる。

2　システム管理者またはシステム管理者が指定した職員以外は、サーバー等の機器操作又は情報シスシステムへのアクセスを行つてはならない。

3　システム管理者は、サーバー等の情報システムの操作に関する認証機能を設定し、パスワード等の管理に関する定めの整備(その定期又は随時の見直しを含む。)及びパスワードの読取防止に必要な措置を講ずるものとする。

4　システム管理者は、災害等に備え、サーバー等の機器の予備電源確保、配線損傷防止等、必要な措置を講ずるものとする。

## 第６章 保有個人情報の提供及び業務の委託等

(保有個人情報の提供)

第２９条　保護管理者は、第三者に保有個人情報を提供する場合には、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わし、安全確保の措置を要求するとともに、必要に応じて、提供前又は随時に実地の調査等を行うことにより、当該措置状況の確認を行い、その結果を記録し、改善要求等の措置を講ずるものとする。

（業務の委託等）

第３０条　保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講ずるものとする。また、契約書に次に掲げる事項を明記するとともに、委託先における責任者等の管理体制、個人情報の管理の状況についての検査に関する事項等の必要な事項ついて書面で確認するものとする。

(1) 個人情報に関する秘密保持等の義務

(2) 再委託の制限又は条件に関する事項

(3) 個人情報の複製等の制限に関する事項

(4) 個人情報の漏えい等の事案の発生時における対応に関する事項

(5) 委託終了時における個人情報の消去及び媒体の返却に関する事項

(6) 違反した場合における契約解除の措置その他必要な事項

2　保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記するものとする。

## 第７章 安全確保上の問題への対応

(事案の報告及び再発防止措置)

第３１条　保有個人情報の漏えい等、安全確保の上で問題となる事案が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する保護管理者及びシステム管理者に報告する。

2　保護管理者及びシステム管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。

3　保護管理者及びシステム管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。但し、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に事案の内容等について報告する。

4　総括保護管理者は、上記第３項の規定に基づく報告を受けた場合には、事案の内容等に応じて、その事案の内容、経緯、被害状況等を会長に速やかに報告する。

5　総括保護管理者は、保護管理者及びシステム管理者とともに、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。

（公表等）

第３２条　総括保護管理者は、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずるものとする。

## 第８章 監査及び点検の実施

(監査)

第３３条　監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査(外部監査の委託を含む。)を行い、その結果を総括保護管理者に報告するものとする。

(点検)

第３４条　保護管理者及びシステム管理者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告するものとする。管理者に報告するものとする。

(評価及び見直し)

第３５条　保有個人情報の適切な管理のための措置については、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

## 第９章 補足

（他の法令との関係）

第３６条　法令の規定により、個人情報の管理に関する事項について特別の定めが設けられている場合においては、当該事項については、当該法令の定めるところによるものとする。

（細則）

第３７条　本規程の施行に関し必要な事項は、別に総括保護管理者が定める。

２　保護管理者及びシステム管理者は、本規程を実施し、又は保有個人情報の適切な管理のため、必要があるときは、細則を定めることができる。

３　保護管理者及びシステム管理者は、前項の細則を定め、変更し、又は廃止したときは、速やかに総括保護管理者に報告しなければならない。

第３８条　当法人の個人情報保護に関する方針は、別に会長が定めるところとする。

附則

１．　本規程の改廃は、理事会の決議を経て行う。

２．　本規程は令和３年(2021 年）２月 16 日から施行するものとし、同年２月 16 日から適用する。